UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/454,865	12/07/1999	SHINICHIRO TANIGUCHI	104934	4339

25944 7590 01/05/2005

OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/454,865	TANIGUCHI ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *9/29/2004* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 9/29/2004, Applicant amends the independent claims 1, 13, 16-18, 20-27 to further limit the claim invention. The following claims 1-27 are presented for examination.

2. Applicant's arguments, see pages 17-21, filed on 10/28/2003, with respect to the rejection of claims 1-27, have been fully considered, but are moot in view of a new ground of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.1 **Claims 1-27** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,117,096 to **Bauer et al.** in view of US Patent Publication US 2002/0013898 to **Sudia et al.**

3.2 **As per claims 1, 10, 11, and 12, Bauer et al.** substantially teaches a distribution information management system having a structure comprising a control and monitoring unit connected with the goods to be distributed with sensors and actuators for storing state of distribution process that meets the recitation of a data carrier attached to an article for storing the information of the article (see column 2, lines 10-24), the distribution information processing module comprising: a reading part and storing part that reads out data of the data carrier and stores information in the data carrier, for example (see column 6, lines 18-25) and interface that meets the recitation of a first communication part that communicates with the distribution information management module (see figure 1); an information generating unit that processes the information to be stored in the data carrier wherein the information includes at least a signer identifier that is a receiver identifier of last information stored in the data carrier, for example (see column 5, line 66 through column 6, line 15 and column 5, lines 9-21). **Bauer et al.** substantially discloses a memory card for read write access and suggests using access code that meets the recitation of a first information verification unit comprising a first part that verifies the information read out from the data carrier a first verification key storage part that stores the verification key used by the first information verification part for verification of the information, for example (see column 2, lines 15-25 and column 6, lines 25-55), an information generating unit that processes the information to be stored in the data carrier comprising: a distribution information generating part that generates the information to be stored in the data carrier (see column 6, lines 60-65).

Bauer et al. discloses a programmable card as well as an analysis unit for verifying all transactions during the distribution process, for example (see column 2, line 47 through column 3, line 35) and discloses each unit comprising computer and interfacing with the memory card and capable of interfacing with each other (see figure 1). Although **Bauer et al.** some security with access code etc., **Bauer et al.** does not explicitly disclose a signature generating process that stores signature key information for generating a digital signature. However, **Sudia et al** in an analogous art discloses a distribution verification system that is able to sign and verify the signature of the sender comprising first verification key storage part that stores the verification key used by the first information verification part for verification of the information, for example (see page 3, paragraphs 0047-0048), a signature module that performs signature generating process, for example (see page 4, paragraph 0054); a signature key storage part that stores the signature key information used by the signature module for generating a digital signature, for example (see page 4, paragraphs 0054-0055); **Sudia et al** discloses that each signing device and each authorizing agent has set of public and signature verification keys of other devices (page 5, paragraph 0066), and suggests that keys will be selected or acquired from the stored keys (page 4, paragraph 0050) that meets the recitation of a signature key information selection part; that selects a signature key information stored in the signature key storage part; a signature key information acquisition part that acquires the signature key information from the distribution information management module, for example (see page 4, paragraph 0050); the signature module comprising: a signature part that generates a digital signature for the information generated by the distribution information generating part, for example (see page 4, paragraphs 0054-0055); and a first signer private information storage part that stores signer private

information used by the signature part for generating a digital signature, for example (see page 4, paragraphs 0054-0055); **Sudia et al** suggests interaction between devices and a signature key information generating part that generates a signature key information used by the distribution information processing module, for example (see page 5, paragraphs 0067-0072) **Sudia et al** adds that the verification process disclosed offers several advantages in preventing tampering (page 4, paragraph 0053) including applying a signature and at the same time verifying the signature of the sender and with improved security and flexibility (see page 1, paragraphs 0006 and 0012). Therefore, it would have been obvious to one skilled in the art at the time the invention was made to modify the system of **Bauer et al.** to provide a key signature verification process as taught by **Sudia et al** capable of generating, storing, selecting key, and verifying signature of the sender. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Sudia et al** so as to provide an improved signature verification process that can detect unauthorized verifiers and signers with increased security and flexibility, for example (see page 1, paragraphs 0006 and 0012).

Bauer et al. further discloses the distribution information management module comprising: interface that meets the recitation of a second communication part that communicates with the distribution information processing module, for example (see column 6, lines 35-50); a second information verification unit that processes the information received comprising: a second information verification part that verifies the information received from the distribution information processing module, for example (see column 6, lines 42-65). **Sudia et al** discloses signing device and authorizing agent that can perform the same function as discussed above (see page 5, paragraph 0057); therefore, **Sudia et al** also discloses a second verification

key storage part that stores the verification key used by the second information verification part for verification of the information (see page 5, paragraph 0066); a signature key information generating part that generates a digital signature key information used by the distribution information processing module for generating a distribution information, for example (see page 5, paragraph 0069); a signature key storage part and a signer private information selection part that selects signer private information used by the signature key information generating part for generating signature key information (see page 4, paragraphs 0054-0055); and a second signer private information storage part that stores the signer private information (see page 5, paragraphs 0066 and 0072). Therefore, it would have been obvious to one skilled in the art at the time the invention was made to modify the system of **Bauer et al.** to provide a second key signature verification unit as taught by **Sudia et al** capable of generating, storing, selecting key, and verifying signature of the sender. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Sudia et al.** so as to provide an improved signature verification process that can detect unauthorized verifiers and signers with increased security and flexibility, for example (see page 1, paragraphs 0006 and 0012).

As per claims 2-3, both references suggest using a smart card for verification process that can be detachable from other units. **Sudia et al** discloses using a smart card that is tamperproof that meets the recitation of wherein the signature module is tamperproof and detachable from the distribution information processing module (see page 4, paragraphs 0054-0055). Therefore, claim 2 is rejected on the same rationale as the rejection of claim 1.

As per claim 4, Bauer et al. discloses the claimed system of claim 1 but does not disclose the limitation wherein the information generating unit has a signature key use limit information storage part that limits a specified number times for signatures performed using the signature key, the signature key information selection part does not select signature key information used more than a specified number of times for signature. It is well known in the art program that limits and revokes number of times of performing password or using keys. **Sudia et al** discloses limiting use of key signature and key revocation that meets the recitation of a signature key use limit information storage part that limits a specified number times for signatures performed using the signature key, the signature key information selection part does not select signature key information used more than a specified number of times for signature, for example (see page 5, paragraphs 0056, and page 6, paragraph 0075, and page 7, paragraphs 0014-0115 and page 13, paragraph 0197). Therefore it would have been obvious to one skilled in the art at the time the invention was made to modify the system of **Bauer et al.** to limit a specified number times for signatures performed using the signature key, not selecting signature key information used more than a specified number of times for signature as suggested by **Sudia et al**. This modification would have been obvious because one skilled in the art would have been motivated to do so in order to protect keys from susceptible attacks as suggested by **Sudia et al** (see page 7, paragraphs 0014-0115).

As per claim 5, Sudia et al discloses the limitation of wherein the signature key use limit information storage part is disposed in the signature module (see page 7, paragraphs 0014-0115). Therefore, claim 5 is rejected on the same rationale as the rejection of claim 4.

Claim 6 has the same limitation as claim 1 except for adding a second reading and storage part in the information generating module. **Bauer et al.** discloses more than one unit with reading/writing means to read and store the information in the data carrier (see column 2, lines 10-40 and column 3, lines 25-45 and column 4, lines 1-12).

Claim 7 has the same limitation as the rejected claim 1 except for adding a third communication part. **Bauer et al.** discloses many interfaces between the units (see figure 1). Therefore, **claim 7** is rejected on the same rationale as the rejection of **claim 1**.

As per claim 8, Sudia et al discloses the limitation of wherein the verification key stored in the first verification key storage part and the second verification storage part is common for all the distribution information processing modules and distribution information modules, for example (see page 3, paragraph 0048). Therefore, **claim 8** is rejected on the same rationale as the rejection of **claim 1**.

As per claim 9, Sudia et al discloses signing device and authorizing agent that can perform the same function as discussed above (see page 5, paragraph 0057).

As per claim 13, Bauer et al. discloses the limitation wherein the information stored in the data carrier comprises at least a product identifier, an identifier of a receiver at a destination of the article and access coding, and which information is stored as one unit (see column 6, lines 1-25 and column 4, line 67 through column 5, line 22). **Bauer et al.** des not explicitly disclose a signature value, but discloses using a data carrier for documenting the originator or addressee and the transfer of responsibility for the transport and control operations during the whole course of distribution (column 2, lines 46-67). However, **Sudia et al** discloses appending signature value to verify the sender, for example (see page 4, paragraph 0055). Therefore it would have been obvious to one skilled in the art at the time the invention was made to modify the system of **Bauer et al.** to add a signature value to the data carrier so as to authenticate the originator or sender and to prevent tampering. This modification would have been obvious because one skilled in the art would have been motivated to do so in order to have further control of authorization during the distribution process as suggested by **Sudia et al** (see page 1, paragraph 0012).

As per claim 14, Bauer et al. suggests maintaining proof concerning the course of the transport and discloses a data carrier for holding all information during the course of the distribution process for replacing transport papers (see column 2, lines 47-60 and column 1, lines 49-62). **Sudia et al** discloses the limitation of wherein the information stored in the data carrier contains at least a verification key identifier, and which information is stored as one unit (see page 6, paragraph 0078). Therefore claim 14 is rejected on the same rationale as the rejection of claims 1 and 13.

As per claim 15, Bauer et al. discloses the limitation wherein the information stored in the data carrier contains at least a distribution information management module identifier, and which information is stored as one unit (see column 6, lines 1-12).

As per claim 16, Bauer et al. discloses the limitation wherein the information stored in the data carrier as one unit contains at least a product identifier, an identifier of a receiver at a destination of the article and access coding that can be separately from the information for unit. **Bauer et al** discloses a data carrier with different units, it is obvious to one skilled in the art that the signature value can be stored separately from the other information. (see column 6, lines 1-12 and lines 25-37). **Sudia et al** discloses using signature value to verify the sender, for example (see page 4, paragraph 0055) as discussed in claim 13 above. Claim 16 is rejected on the same rationale as the rejection of claims 1 and 13.

As per claim 17, Bauer et al. discloses the limitation wherein the information stored in the data carrier contains at least a product identifier, an identifier of a receiver at a destination of the article and a verification key identifier and which information is stored as one unit, and identification code that indicates each verifier that meets the recitation of the information has a signature value corresponding to the verification key identifier for each verification identifier (see column 3, lines 9-26 and column 5, lines 1-11; column 5, line 65 through column 6, line 37). **Bauer et al.** discloses continuous proof and monitoring throughout the transport (see column 1, lines 49 et seq. and column 2, lines 15-24). **Sudia et al** discloses wherein the information stored

in the data carrier contains at least a product identifier, an identifier of a receiver at a destination of the article and a verification key identifier and which information is stored as one unit, and the information has a signature value corresponding to the verification key identifier for each verification identifier (see page 6, paragraph 0078). Claim 17 is rejected on the same rationale as the rejection of claims 1 and 13.

As per claim 18, Bauer et al. discloses a data carrier attached to an article for storing information of the article that stores (see column 4, lines 46 et seq.): distribution information generated for each one or one set of transaction in the distribution process of the article, wherein the distribution information includes at least a signer identifier that is a receiver identifier of last information stored in the data carrier; and at least a part of a signature value of at least part of a piece of the distribution information or at least part of each of serial pieces of the distribution information (see column 5, lines 1-22 and column 5, line 65 through column 6, line 37). Claim 18 contains similar limitation as claims 1 and 13 and therefore is rejected on the same rationale as the rejection of claims 1 and 13.

As per claim 19, Bauer et al. discloses the limitation wherein the distribution information of the article contains at least an identifier of the article, an identifier of the receiver who received the article, and identification code that indicates each verifier that meets the recitation of identifier of the signer who generates the signature value (see column 5, line 65 through column 6, line 37). **Sudia et al** discloses an identifier of the receiver who received the

article, and the identifier of the signer who generates the signature value (see page 6, paragraphs 0078 and 0080) as discussed in claim 13.

Claims 20-23 are similar to the rejected claim 1 except for incorporating the claimed system into a module and a method. Therefore, **claims 20-23** are rejected on the same rationale as the rejection of claim 1.

Claims 24-25 have the same limitation as the rejected claim 1 except for incorporating the claimed system into a computer program product. Therefore, **claims 26-27** are rejected on the same rationale as the rejection of claim 1.

Claims 26-27 have the same limitation as the rejected claim 1. Therefore, **claims 26-27** are rejected on the same rationale as the rejection of claim 1.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses a distribution system with key signature verification where each verifier can generate own signature.

US Patents : 5,661,803, 5982,896 to Cordery et al 5,5444,086 Davis et al

6,005,945 Whitehouse

US Patent Publication : US 2001/0044780 Miyazaki et al.

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Carl Colin

Patent Examiner

December 29, 2004